REMARKS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1-4, 6-14, 16-19, 21-23, 25, and 26 are pending in this application. Claims 1-4, 9, 14, 16, 18, 19, 21-23, and 26 are amended by the present amendment.

Amendments to the claims finds support in the application as originally filed, at least in the specification at page 21, lines 18-26 and Applicants' Figure 5. Thus, no new matter is added.

In the outstanding Office Action dated February 19, 2009, Claims 4, 14, 19, and 23 were objected to; Claims 2, 4, 9-11, and 16 were rejected under 35 U.S.C. § 112, second paragraph; Claims 4, 14, 19, and 23 were rejected under 35 U.S.C. § 101; and Claims 1-4, 6-14, 16-19, 21-23, 25, and 26 were rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Publication 2002/0012433 to Haverinen et al. (herein "Haverinen") in view of U.S. Patent 7,058,414 to Rofheart et al. (herein "Rofheart").

Regarding the objection to the claims, Claims 4, 14, 19, and 23 are amended to recite "[a] computer program storage medium storing computer program instructions . . .". It is respectfully submitted that a computer program storage medium finds support in the written description of the specification at least at page 44, lines 20-23. Thus, it is respectfully requested the objection to the claims be withdrawn.

Furthermore, regarding the rejection under 35 U.S.C. § 112, second paragraph, Claims 2, 4, 9-11, and 16 are amended to correct the minor inconsistencies noted in the Office Action. Therefore, it is respectfully requested that rejection be withdrawn.

Additionally, regarding the rejection under 35 U.S.C. § 101, as noted above, Claims 4, 14, 19, and 23 are amended to recite a computer program storage medium storing computer program instructions. Furthermore, as noted in Applicants' specification, tangible computer

readable media such as a ROM, a hard disk, a magnetic disk, an optical disk, a magnetic optical disk, and a semiconductor memory are non-limiting examples of a computer program storage medium. Furthermore, it is respectfully submitted that a computer program storage medium corresponds to a patent eligible "machine" under 35 U.S.C. § 101. Therefore, it is respectfully requested that rejection also be withdrawn.

In addition, Applicants respectfully traverse the rejection of Claims 1-4, 6-14, 16-19, 21-23, 25, and 26 under 35 U.S.C. § 103(a) as unpatentable over Haverinen and Rofheart.

Claim 1 is directed to a data transmitting apparatus that includes, in part, an expected value generation unit configured to generate an expected authentication value based on shared data shared with a data receiving apparatus and also based on a sequence number. The sequence number indicates a position of a response request command in a sequence of response request commands to be transmitted to a data receiving apparatus.

As noted in Applicant's specification, generation of an expected authentication value based on shared data and a sequence number indicating a position of a command in a sequence of commands may advantageously make it impossible for a receiving terminal to transmit a response message until after the command is received from the transmitting side terminal. Therefore, it is advantageously possible to prevent an illegal act such as transmitting a response message before a command is received to deceptively shorten a response time.[1]

Applicants respectfully submit that the references in the Office Action fail to teach or suggest each of the features of independent Claims 1, 3, 4, 16, 18, 19, 21-23, and 26. For example, Applicants respectfully submit that Haverinen and Rofheart fail to teach or suggest a data transmitting apparatus or method or a receiving apparatus or method in which an expected value generation unit may generate an expected authentication value based on

[1] Specification at page 26, lines 7-13.

shared data shared with a data receiving apparatus and a sequence number indicating a position of a response request command in a sequence of response request commands.

Haverinen describes authentication in a packet data network in which a shared secret is arranged between a mobile node and a telecommunications network authentication center.[2] According to Haverinen, the packet data network forms a session key using authentication triplets and sends to the mobile node challenges and a cryptographic authenticator made by using the session key, and the mobile node forms the rest of the authentication triplets using the challenges and then forms the session key.[3] Additionally, Haverinen indicates that the packet data network may send a challenge and cryptographic information to a mobile node and may receive a response from the mobile node, and then may subsequently verify the response using a session secret.[4] In addition, Haverinen indicates that a default algorithm for authentication calculates an authentication digest for a message by running an MD5 algorithm over a stream of bytes that includes a first occurrence of a key K, protected fields from a registration request, and a second occurrence of the key K.[5] However, Applicants respectfully submit that Haverinen is silent regarding an expected value generation unit that generates an expected authentication value based on shared data and a sequence number indicating a position of a response request command in a sequence of response request commands.

Also, it is respectfully submitted that Rofheart fails to supply the teachings lacking in the disclosure of Haverinen. For example, Rofheart describes a method and system for enabling device functions based on distance information, for example a distance between a local device and a remote device determined based on a time between the transmitting of a

[2] Haverinen at Abstract.
[3] Haverinen at Abstract.
[4] Haverinen at paragraphs [0061]-[0063].
[5] Haverinen at paragraph [0197].

message and the receiving of the response.[6] However, it is respectfully submitted that Rofheart also fails to teach or suggest generating an expected authentication value based on shared data and a sequence number.

Accordingly, Applicants respectfully submit that Haverinen and Rofheart, whether taken individually or in combination, fail to teach or suggest "an expected value generation unit configured to generate an expected authentication value based on the shared data and a sequence number, the sequence number indicating a position of the response request command and a sequence of response request commands to be transmitted by the command transmission unit," as recited in Claim 1.

For similar reasons to those noted above with regard to Claim 1, Applicants respectfully submit that Haverinen and Rofheart also fail to teach or otherwise suggest "generating an expected authentication value based on the shared data and a sequence number, the sequence number indicating a position of the response request command in a sequence of response request commands to be transmitted to the data receiving apparatus," as recited in Claim 3; "controlling generation of an expected authentication value based on the shared data and a sequence number, the sequence number indicating a position of the command in a sequence of commands to be transmitted to the data receiving apparatus," as recited in Claim 4; "an authentication data generation unit configured to generate command authentication data and response expected value data from shared data shared with a data receiving apparatus and a sequence number, the sequence number indicating a position of a response request command in a sequence of response request commands to be transmitted to said data receiving apparatus," as recited in Claims 16 and 26; "generating command authentication data and response expected value data from shared data shared with a data receiving apparatus and a sequence number, the sequence number indicating a position of a

[6] Rofheart at Abstract.

response request command in a sequence of response request commands to be transmitted to the data receiving apparatus," as recited in Claims 18 and 19; "a generating unit configured to generate command expected value data and response authentication data from shared data shared with said data transmitting apparatus and a sequence number, the sequence number indicating a position of the response message in a sequence of response messages to be transmitted to the data transmitting apparatus," as recited in Claim 21; and "generating command expected value data and response authentication data from shared data shared with said data transmitting apparatus and a sequence number, the sequence number indicating a position of the response message in a sequence of response messages to be transmitted to said data transmitting apparatus," as recited in Claims 22 and 23.

Therefore, Applicants respectfully submit that independent Claims 1, 3, 4, 16, 18, 19, 21-23, and 26, and claims depending therefrom, patentably define over Haverinen and Rofheart.

In addition, Applicants respectfully submit that the references in the Office Action fail to teach or suggest the features of independent Claims 6, 13, 14, and 25. Furthermore, Applicants respectfully traverse the assertions in the Office Action to the contrary, for example at page 9, lines 12-15. In particular, it is respectfully submitted that Haverinen paragraph [0062] fails to teach "a response message generation unit configured to generate the response message to said response request command ***before*** said response request command is received from said data transmitting apparatus," as asserted by the Office Action.[7]

Claim 6 is directed to a data receiving apparatus that is configured to receive data from a data transmitting apparatus. The data receiving apparatus of Claim 6 includes, in part, an authentication data generation unit configured to generate authentication data ***before*** a

[7] Office Action at page 9, lines 12-15.

response request command requesting transmission of the authentication data is received from the data transmitting apparatus.

Applicants discovered that since the authentication data and the response message assembled with the authentication data is generated ***before*** the response request command is received, a reception side terminal can advantageously return a response message to a transmission side terminal immediately after a response request command is received.[8]

Haverinen describes a communication between a foreign server FAAA and a home server HAAA.[9] According to Haverinen, in a step 8, the FAAA (e.g., data transmitting apparatus) sends a SIGNsres (e.g., response request command) to the home server HAAA (e.g., data receiving apparatus).[10] Furthermore, Haverinen teaches that subsequently, in a step 9, the HAAA (e.g., receiving apparatus) verifies that the SIGNsres is valid by checking the received SIGNsres against the output of a hash function HASH2 (e.g., authentication data).[11] In other words, according to Haverinen, authentication data is generated at a receiving apparatus ***after*** a response request command is received from a data transmitting apparatus.

Accordingly, Applicants respectfully submit that Haverinen fails to teach or suggest "an authentication data generation unit configured to generate said authentication data based on shared data shared with the data transmitting apparatus by subjecting said shared data to a predetermined process before said response request command is received from said data transmitting apparatus," as recited in independent Claim 6, and as similarly recited in independent Claims 13, 14, and 25. Furthermore, it is respectfully submitted that Rofheart also fails to teach or suggest the claimed features lacking in the disclosure of Haverinen.

---

[8] Specification at page 26, lines 14-18.
[9] Haverinen at paragraph [0174].
[10] Haverinen at paragraph [0185].
[11] Haverinen at paragraph [0186].

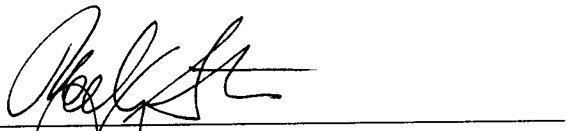
Therefore, it is respectfully submitted that independent Claims 6, 13, 14, and 25 also patentably define over Haverinen and Rofheart.

Accordingly, Applicants respectfully submit that independent Claims 1, 3, 4, 6, 13, 14, 16, 18, 19, 21, 22, 23, 25, and 26, and the claims depending therefrom, are allowable.

Consequently, in light of the above discussion and in view of the present amendment this application is believed to be in condition for allowance and an early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Zachary S. Stern
Registration No. 54,719

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413-2220
(OSMMN 06/04)